(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 227 318**
A3

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: **86309231.8**

(51) Int. Cl.4: **H04L 9/02**

(22) Date of filing: **26.11.86**

(30) Priority: **30.11.85 JP 268321/85**
30.11.85 JP 268322/85

(43) Date of publication of application:
01.07.87 Bulletin 87/27

(84) Designated Contracting States:
DE FR GB NL SE

(88) Date of deferred publication of the search report:
22.02.89 Bulletin 89/08

(71) Applicant: **NEC CORPORATION**
33-1, Shiba 5-chome, Minato-ku
Tokyo 108(JP)

(72) Inventor: **Kage, Kouzou**
NEC Corporation 33-1 Shiba 5-chome
Minato-ku Tokyo(JP)

(74) Representative: **Orchard, Oliver John**
JOHN ORCHARD & CO. Staple Inn Buildings
North High Holborn
London WC1V 7PZ(GB)

(54) **Encryption/decryption system.**

(57) An encryption/decryption system for a communication channel increases the number of values for the encryption key variable without increasing the length of a cipher feedback register. This is done by providing a selector (13) to select one from many local and prestored keys for each frame. The transmitting end has a first storage register (12), a first memory (22), a first selector (13), and an encrypting circuit (10). The encrypting circuit combines a randomized signal with the input signal to form an encrypted signal. As cipher feedback, the first storage register (12) provides bits of the encrypted signal as addresses to the first memory (22), which outputs corresponding random numbers. The first selector (13) selects from the random number data to form the coding randomized signal fed to the encrypting circuit. The receiving end has a second storage register, a second memory, a second selector, and a digital signal decoding circuit. The second storage register stores bits of a received encrypted signal and outputs them in parallel as addresses. The second memory receives these addresses and outputs corresponding random numbers. To enable decoding, the working and stored contents of the first and second memories are identical. The second selector, operating the same way that the first operates, selects from the identical random number data to form a decoding randomized signal. The decoding circuit combines the received encrypted signal with the decoding randomized signal to reproduce the input digital signal.

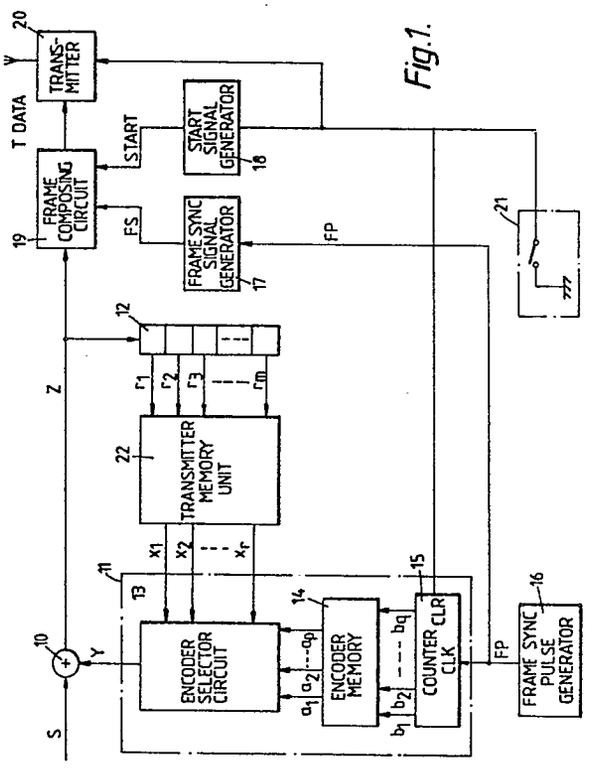

Fig.1.

EP 0 227 318 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 86 30 9231

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.4)
A	US-A-4 447 672 (NAKAMURA) * Column 4, line 14 - column 5, line 30; figure 1 * ---	1,3,5	H 04 L 9/02
A	IEE PROCEEDINGS SECTION A A I, vol. 129, no. 6, part A, August 1982, pages 357-376, Old Woking, Surrey, GB; H.J. BEKER et al.: "Communications security: A survey of cryptography" * Figure 15 * ---	1-5	
A	US-A-4 176 247 (ENGLUND) * Column 1, line 63 - column 3, line 32; figures 1,2 * ---	1,3,5	
A	PATENT ABSTRACTS OF JAPAN, vol. 9, no. 136 (E-320)[1859], 12th June 1985; & JP-A-60 20 660 (SHARP K.K.) 01-02-1985 * Abstract * ---	5,6,8	
A	GB-A-2 151 886 (B.B.C.) * Abstract; figure 7 * ---	1-5,8	TECHNICAL FIELDS SEARCHED (Int. Cl.4)
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 14, no. 10, March 1972, pages 2978-2979, New York, US; R.O. SKATRUD: "Random-key generator for ciphering system" * Whole article * -----	1-5,8	H 04 L H 04 K

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	24-11-1988	SNELL T.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)